0400

Docket No.: 1573.1010

#3

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re the Application of:

Koichi ITO, et al.

Serial No. 10/028,265 ✓ Group Art Unit:

Confirmation No.

Filed: December 28, 2001 Examiner:

For: ENCRYPTION SECURED AGAINST DPA

PRELIMINARY AMENDMENT

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

Before examination, please amend the above-identified application, as follows:

IN THE SPECIFICATION:

Please REPLACE the paragraph beginning at page 8, line 30, as follows:

When the conventional encrypting process in which the conventional key XOR function, the linear function, and the nonlinear function as shown in FIGURES 2, 3 and 4 are used is changed to the encrypting process shown in FIGURE 10, they are replaced with a key XOR function, a linear function, and a nonlinear function as shown in FIGURES 11, 12 and 13A, respectively, in accordance with the random mask value method.

Please REPLACE the paragraph beginning at page 9, line 1, as follows:

In the random mask value method, the computation of the conventional intermediate data X_i in the encryption is replaced with the computation of the X_i' and the random number R_i which satisfy the exclusive OR, $X_i = X_i'$ XOR R_i. The encrypting unit computes X_i', and the mask value generating unit computes R_i. The following equations (7) are established for X_i, X_i', Z_i, Z_i', R_i, and RO_i in the operations shown in FIGURES 2 and 11, FIGURES 3 and 12, and FIGURES 4 and 13A.